Information and Communication Technology Security

Information Security Policy

October 2023

FUNDACIÓN COMPLUTENSE

INFORMATION AND COMMUNICATIONS TECHNOLOGY SECURITY

PREPARED BY:	REVIEWED BY:	APPROVED BY:
Babel Group	Head of Security and DPO	Directorate General of the FGUCM
signature:	signature:	signature:

CHANGE HISTORY

FILE NAME	Version	SUMMARY OF CHANGES	Date
FGUCM STIC-POL - Information Security Policy v1.0.docx	1.0	First edition of the document	14/04/2023
FGUCM STIC-POL - Information Security Policy v1.1.docx	1.1		01/10/2023

DOCUMENT CLASSIFICATION

INTERNAL USE

Confidentiality notice: The information contained in this document is for INTERNAL USE ONLY and may only be used in accordance with the DISTRIBUTION CONTROL clause.

It is the responsibility of the Area or Department receiving this document to distribute it internally based on the need to know the information contained herein.

DISTRIBUTION CONTROL

AUTHOR(S): Babel Group

DISTRIBUTION: GENERAL FOUNDATION OF THE COMPLUTENSE UNIVERSITY OF MADRID (FGUCM)

References

INTERNAL DOCUMENTS	
1.1 Title	**FILE NAME**
[1] FGUCM Regulatory Framework	FGUCM STIC-POL - Regulatory Framework v1.00.docx
EXTERNAL DOCUMENTS	
[1] CCN-STIC-801 ENS. Responsibilities and functions	
[2] CCN-STIC-805 ENS-Information Security Policy	
[3] CCN-STIC-402: Organisation and Management for the Security of ICT Systems. 2006	
[4] Royal Decree 311/2022, dated 3 May, regulating the National Security Scheme	
[5] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)	
[6] Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights	
[7] ISO/EIC ISO 27001 Information security, cybersecurity and privacy protection - Information security management systems - Requirements	

COMPLIANCE	
NSS	GDPR
org.1 Security policy	

CONTENTS

1. Introduction

This document constitutes the Information Security Policy of the **GENERAL FOUNDATION OF THE COMPLUTENSE UNIVERSITY OF MADRID (FGUCM)**, as set out in Article 12 of Royal Decree 311/2022, dated 3 May, which regulates the National Security Scheme, and which establishes the minimum Security requirements in the field of Electronic Administration, and the organic security measure 1 provided for in Annex II of said Royal Decree.

In this regard, the aforementioned Article 12, in its second paragraph, establishes that '*Each public administration must have a security policy formally approved by the competent body. Likewise, each body or entity with its own legal personality included in the subject matter scope of Article 2 must have a security policy formally approved by the competent body'.*

The structure of this document follows the guidelines established by the CCN-STIC-805 guide for drafting the Information Security Policy within the scope of the National Security Scheme.

The Information Security Policy sets out the FGUCM's position on information security and establishes the general criteria that should govern the organisation's activities in terms of security.

The objective of Information Security is to guarantee the quality of information and the continued provision of services, while acting preventively, monitoring daily activity and promptly reacting to incidents.

Information systems must be protected against rapidly evolving threats that have the potential to impact the availability, integrity, confidentiality, authenticity, traceability, intended use and value of information and services. Defending against these threats requires a strategy that adapts to evolving surrounding conditions in order to ensure the continued delivery of services.

This means that it is necessary to apply the Clauses of the ISO/IEC 27001 standard, the security measures required by the National Security Scheme, Regulation (EU) 2016/679 General Data Protection Regulation and Organic Law 3/2018, dated 5 December, on the Protection of Personal Data and guarantee of digital rights (hereinafter SGSI, ENS, RGPD and LOPDGDD). It is also necessary to continuously monitor the levels of service provision, track and analyse reported vulnerabilities, and prepare an effective response to incidents to ensure the continuity of the services provided.

2. The General Foundation of the Complutense University of Madrid (FGUCM)

The General Foundation is a non-profit institution, established in 1984 as a result of the merger of eighteen Foundations of the Complutense University of Madrid (UCM). The merger came about because of private donations of both money and property. The FGUCM's objectives and goals match those of the UCM, and so its essential activities are related to the management of research and education and the transfer of knowledge. It funds its activities mostly from public sources and also receives funding from private institutions.

3. Regulatory Framework

This policy is framed within the regulatory framework specified in the document *Regulatory Framework of the FGUCM*.

4. General Security Policy

The purpose of this Policy is to establish the position of the FGUCM regarding Security that affects the processes related to the performance of its functions and, specifically, processes related to electronic administration. The policy addresses both the external perspective (from the users of the services) and the internal point of view, which relates to the management of the Entity itself.

FGUCM uses Information and Communications Technologies (ICT) to provide its services, and is therefore aware that these systems must be managed diligently. In doing so, appropriate measures must be taken to protect the systems from accidental or deliberate harm.

Likewise, it is also aware that security incidents can be caused from remote locations, through connections to available communications networks and, especially, through connections to the Internet (cyberattacks).

The policy of the FGUCM is to counteract the aforementioned threats with sufficient means, within the bounds of economic feasibility. To this end, a security structure will be established, along with the appropriate mechanisms to manage it, and a set of support instruments to ensure:

- the fulfilment of its mission and service delivery objectives.
- compliance with applicable laws and regulations.

To do this,

- Measures will be provided for and deployed to avoid security incidents that could affect the achievement of objectives or put information at risk.
- Response measures will be designed for security incidents, whether physical or logical, in such a way as to minimise their impact, should they occur.

As a general rule, a risk-oriented approach will be taken when designing the necessary security measures, putting more focus and effort into mitigating whatever represents a greater risk.

The different areas under whose responsibility the services provided lie must consider security from the moment a new system or service is conceived. The responsible areas must apply the security measures prescribed by the National Security Scheme to those new systems and services and to existing ones with the goal of guaranteeing the availability, confidentiality, integrity, authenticity and traceability of the services and information.

System security requirements, the training needs of users, administrators and operators, and funding needs must be identified and included in system planning and in the specification sheets used to implement projects involving ICT.

Prevention, response and recovery mechanisms must be put in place to minimise the impact of security incidents.

As for Prevention, services and information must be prevented from being affected by a security incident. To this end, the FGUCM will implement the security measures established in Annex II of the ENS, as well as additional measures that may be identified in the risk analysis process.

As for Detection, mechanisms for the detection, communication and management of security incidents will be established, so that any incident can be dealt with as quickly as possible. Whenever possible, security incidents will be detected automatically through service monitoring or anomaly detection elements, and incident response procedures will be implemented as quickly as possible. For incidents detected by users, whether internal or external, the relevant incident communication channels will be established.

As for Response, measures will be established that will be implemented at the appropriate time and will be aimed at restoring information and services that may have been affected by a security incident. For those services considered critical as per the assessment of the persons responsible for them, plans must be developed that allow for the continuity of said services in the event that, as a result of a security incident, they become unavailable.

As for Conservation, the information system will guarantee the conservation of data and information in electronic format once the security incident has been resolved.

5. Scope

This Information Security Policy applies to all services provided by FGUCM that are supported by Information and Communication Technologies, as well as to all staff, without exception.

6. Information security organisation

Security in the FGUCM is supported by the structures and roles described below:

- Specification structure, which is responsible for establishing the security requirements associated with the services provided.
- Supervisory structure, which is responsible for verifying compliance with security requirements and ongoing alignment with the organisation's objectives.
- Operation structure, which is responsible for implementing the identified security measures.

6.1 Specification structure

This structure is responsible for determining the security requirements that will apply to the services provided by the FGUCM and ensuring compliance with the associated regulations that apply to it, specifically Royal Decree 311/2022, dated 3 May, which regulates the National Security Scheme.

The following are part of this structure:

- Information and Service Managers.

6.1.1 Information and Service Managers

The Information and Service Managers will establish the level of security that the information and services provided by the FGUCM require. They shall make this assessment based on their requirements regarding availability, confidentiality, integrity, authenticity and traceability, while taking into account the impact that the lack of any of these aspects would have on members of the public and on the Organisation itself.

The Information and Service Managers will be appointed by the Directorate General of the FGUCM.

6.2 Oversight structure

The security oversight structure is responsible for verifying the proper implementation and operation of the security requirements that have been established, in order to maintain alignment with the objectives and to comply with the applicable standards and legislation.

The Information Security Officer is responsible for overall oversight of all activities related to information security.

The Information Security Committee is responsible for organisation-wide and comprehensive coordination of security.

The functions and responsibilities of each of the figures are described in the following sections.

6.2.1 Information Security Officer

Responsible for the definition, coordination, dissemination and verification of the Information Security requirements in the Organisation.

This Officer is part of the Security Committee, in the role of Committee Secretary and, therefore, is responsible for bringing to the Committee matters of interest related to information security.

Their responsibilities include:

- Call meetings of the Security Committee.
- Coordinate and exercise oversight of the Organisation's Information Security and Data Protection measures.
- Supervise the implementation of established standards and procedures and maintain, check and verify compliance with them.
- Ensure that the Organisation's annual ICT security budget is drawn up.
- Define a security management model aligned with the Organisation's security strategy. This management model will be called ISMS (Information Security Management System), regardless of whether the system is based on international standards that offer recommendations or a different model.
- Oversee the practical implementation of the Organisation's Information Security strategy.
- Monitor exceptional cybersecurity situations (or incidents) that occur in the Organisation.
- See to the regular performance of information security risk analyses.
- Request that the Human Resources Department carry out training and awareness-raising programmes on information security.
- Analyse security indicators to measure the effectiveness and efficiency of the measures implemented.
- Analyse information security incidents reflected in these records and verify that plans have been established to resolve them.
- Maintain up-to-date documentation associated with information security management: regulations, procedures and records.
- Authorise in writing the execution of data recovery procedures in cases where required.
- Collaborate with external/internal audits on information security, review them and instruct those responsible for the systems to implement any resulting corrections.

The Information Security Officer will be appointed by the Directorate General of the FGUCM.

6.2.2 Information Security Committee

The mission of the Information Security Committee is the general coordination of activities related to comprehensive information security.

A fundamental objective of the Information Security Committee is to share important information related to security with all persons and organisations responsible. This will prevent the persons with responsibility for activities related to security from being left without sufficient knowledge, or without sufficient support or commitment. Security-related activities may affect several or all areas of the organisation, and a lack of proper support may limit their effectiveness.

The functions of the Security Committee are:

- Regularly report on the security status to the General Directorate of FGUCM.
- Regularly review the Information Security Policy and propose changes, if appropriate.

- Review the internal security regulations that may arise from the Information Security Policy and offer them for approval.
- Develop and propose training requirements for key personnel who handle information, systems and physical infrastructure.
- Offer for approval the security improvement plans that stem from risk analyses carried out.
- Monitor the implementation of approved action plans.
- Coordinate security actions that may be carried out in different areas of the Organisation in order to avoid duplicative or misaligned efforts with the Information Security Policy.
- Analyse significant security incidents and decide how to address them. Some incidents may involve costly action, which would be summitted for approval.
- Analyse information on any security indicators defined. Make decisions in the event of deviation from the established thresholds.
- Propose security solutions that require an approved budget.

The following shall be permanent members of the Information Security Committee:

- Security Manager
- Systems Manager
- Services and Information Manager

Additionally, persons responsible for the specific matters to be discussed at the meetings may attend the Information Security Committee and may be invited depending on the content of the agenda.

6.3 Operation structure

The Security Operation Structure must assume the Operational Administration of the security of information systems. The Structure must also implement in said systems the necessary measures to satisfy the security requirements established by the specification structure.

The functions and responsibilities of the figures associated with the operating structure are described below.

6.3.1 Information System Manager

This manager’s roles and responsibilities are:

- Define, in coordination with the Information Security Manager, the functional security specifications of the Organisation's Information Systems.
- Ensure that the necessary aspects of information security in terms of availability, integrity, confidentiality, authenticity and traceability are taken into account from the outset when designing information systems and communications networks.
- Check that the security settings after installing a new system are adequate.
- Check that security settings remain appropriate after changes to a system.
- Implement and verify the operation of security measures resulting from risk treatment plans or corrective action plans following information security audits.
- Verify the suitability and functionality of information security indicators.
- Conduct periodic technical audits to verify the operation of the measures and compliance with the established security requirements. These audits may be carried out by internal or external personnel of the FGUCM.

The Head of Information Systems will be appointed by the Directorate General of the FGUCM.

7. Functions and obligations

In addition to the functions and powers of the personnel that make up the organisational structure responsible for security, the obligations of the FGUCM personnel, as well as third parties that may have access to its information systems, are set out below.

7.1 Functions and obligations of the staff

All FGUCM personnel who have any kind of relationship with the use, management, maintenance and exploitation of information and the services provided from it, are obliged to be familiar with the Information Security Policy and comply with it. The Information Security Committee will provide the means for this Policy to reach the parties concerned.

All such personnel must attend security awareness sessions, which will be established in the annual training and awareness plan.

Persons responsible for the use, management, maintenance or operation of ICT-supported services will receive training in the secure use of systems, to the extent necessary to perform their work. Training will be mandatory before taking on a responsibility, whether it is the person’s first assignment, a change of job or a change of responsibilities within a job.

7.2 Functions and obligations of third parties

Third parties involved in the management, maintenance or operation of the services provided by FGUCM shall be subject to this Information Security Policy. Third parties shall be bound by this Policy and any regulations derived from it.

Third parties may develop their own operating procedures to comply with the Policy.

Specific incident reporting procedures must be established so that affected third parties can report them.

Third party staff must be given awareness sessions, as is required for in-house staff.

When a third party cannot satisfy any aspect of this Policy, the Information Security Officer must prepare a report on the risk involved. This risk must be accepted by the Information Security Committee.

7.3 Dispute resolution

In the event of a dispute between the different information or service managers that make up the organisational structure of the Information Security Policy, this will be resolved by their hierarchical superior with the mediation of the Information Security Manager. The matter will be referred to the Information Security Committee for resolution if no agreement is reached.

In resolving these disputes, the requirements stemming from the protection of personal data will always be taken into account.

8. Training and awareness

At least one training and awareness-raising action on security matters will be carried out annually.

The objective of the training and awareness-raising action is twofold:

- Keep the personnel most directly involved in information management and the systems that process it informed about existing security procedures, risks, protection measures, protection plans, etc.

- Raise awareness among staff in general about the importance of security and basic procedures for handling and exchanging information.

The first objective is associated with Training and the second with Awareness.

The responsible areas will determine the format of the Training and Awareness action, as well as its content.

9. Risk management

The services and infrastructures within the scope of this Policy must be subject to a risk analysis to guide protection measures to minimise risk.

Magerit will be used as the basic methodology for carrying out risk analyses, as this methodology is the most recommended for the Spanish public sector.

The catalogue of security threats provided in the methodology will be used as a starting point.

The analysis will be carried out:

- On a consistent cycle, once a year.
- When there are significant changes in the information handled.
- When there are changes in the essential services provided or significant changes in the infrastructure that supports them.
- When a serious security incident occurs.
- When severe threats are identified that have not been taken into account or serious vulnerabilities that are not counteracted by the implemented protection measures.

According to the risk scale of the Magerit methodology, the risk level must be below the HIGH level to be considered acceptable in any case (the maximum residual risk must be MEDIUM). Residual risk values greater than MEDIUM must be explicitly accepted by the Information Security Committee, after justifying the appropriateness of their acceptance.

For residual risk values that are not acceptable, the corresponding Treatment Plan must be drawn up to bring the risk values to acceptable levels.

10. Personal data

The FGUCM will apply the principles included in the GDPR when processing personal data:

- Principle of ‘lawfulness, fairness and transparency’: data must be processed in a manner that is lawful, fair and transparent for the party concerned.
- Principle of ‘purpose limitation’: this involves, on the one hand, the obligation that data be processed for one or more specific, explicit and legitimate purposes and, on the other, that data collected for specific, explicit and legitimate purposes are prohibited from being subsequently processed in a manner incompatible with those purposes.
- Principle of ‘data minimisation’: the FGUCM will only collect personal data when they are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Principle of ‘accuracy’: the data must be accurate and, if necessary, up-to-date, and the FGUCM must take all reasonable measures to rectify or delete inaccurate data in relation to the purposes pursued.

- Principle of ‘limitation of the retention period’: only adequate, relevant and necessary data may be processed for a purpose; the retention of such data must be limited in time to the achievement of the purposes pursued by the processing. Once these purposes have been achieved, the data must be deleted or, at a minimum, stripped of any element that allows the parties concerned to be identified.
- Principle of ‘integrity and confidentiality’: obligation to act proactively with the aim of protecting the data they handle against any risk that threatens the data’s security.
- Principle of ‘proactive responsibility’: This means that the FGUCM applies the appropriate technical and organisational measures to guarantee and be able to demonstrate that the processing of personal data is carried out in accordance with the GDPR.

The FGUCM will implement security measures to guarantee the fundamental right to data protection by ensuring the confidentiality, integrity and availability of personal data. To guarantee these three security factors, the FGUCM will apply the necessary security measures to ensure a level of security appropriate to the risks of varying probability and severity for the rights and freedoms of individuals in accordance with Article 32 of the GDPR.

With regard to security measures in the public sector, the FGUCM will comply with the first additional provision of the Organic Law on Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD, by its Spanish initials). This legislation states that data controllers listed in Article 77.1 of the aforementioned organic law who process personal data, which includes public sector foundations such as the FGUCM, must apply the security measures that correspond to those provided for in the National Security Scheme, as well as undertake to ensure that measures followed by companies or foundations linked to those companies and subject to private law are implemented to an equivalent degree.

The FGUCM shall have a Registry of Personal Data Processing Activities that will include the contents regulated in Article 30 of the GDPR and will make that registry public on its transparency portal in application of Article 31.2 of the LOPDGDD.

11. Third parties

When the FGUCM uses services or handles information from third parties, it will make them aware of this Information Security Policy. The Information Security Committee will establish reporting channels and channels for coordinating the respective Security Committees and will establish procedures for reacting to security incidents.

When the FGUCM provides services to other organisations or transfers information to third parties, it will inform them of this Information Security Policy and the Instructions and Procedures that apply to said services or information. Said third party will be subject to the obligations established in said regulations, and may develop its own operating procedures to comply with them. Specific procedures for reporting and resolving incidents will be established. Third party personnel will be required to be adequately aware of security issues, and in any case at least to the same level as that established in this Policy.

Where any aspect of the Policy cannot be satisfied by a third party as required in the preceding paragraphs, a report from the Information Security Officer will be required outlining the risks involved and how they are to be addressed. Approval of this report by the information controllers and affected services will be required before proceeding.

12. Development of the Information Security Policy

This Information Security Policy will be developed through the preparation of other security policies or regulations that address specific issues. Procedures may be developed based on these policies and regulations that describe how to carry them out.

The documentation of security policies and regulations, as well as this Information Security Policy, will be available to all personnel of the organisation who need to know it and, in particular, the personnel who use, operate or manage the information and communications systems or the information itself housed in said systems or the services provided by the FGUCM.

The Information Security Policy is mandatory and is structured in the following hierarchical levels:

1) First level: Information Security Policy.
2) Second level: Information Security Regulations.
3) Third level: Information Security Technical Procedures and Instructions.
4) Fourth level: Reports, records and electronic evidence.

The hierarchical structure allows lower levels to efficiently adapt to changes in the FGUCM operating environments, without the need to review its security strategy.

FGUCM staff will be required to know and comply with all Regulations, Procedures and Technical Instructions on Information Security that may affect their functions, in addition to the Information Security Policy.

The Information Security Policy, Regulations, Procedures and Technical Instructions will be available to all employees on the FGUCM Intranet as they are approved.

1) First level: Information Security Policy

This document is binding on all persons, both internal and external, of the FGUCM, and is included in this document and approved by the Directorate General of the FGUCM.

2) Second level: Information Security Regulations

Mandatory compliance in accordance with the corresponding organisational, technical or legal field.

The responsibility for approving documents drawn up at this level will lie with the Information Security Committee, with the guidance of the Information Security Manager.

3) Third level: Information Security Procedures and Technical Instructions

Technical documents aimed at solving tasks considered critical due to the damage that would be caused by inadequate action. Relevant action may extend to security, development, maintenance and operation of information systems.

The responsibility for approving these technical procedures lies with the manager of the corresponding Information System, under the supervision and guidance of the Information Security Manager.

In the event that the procedures affect several information systems, it will be the responsibility of the Information Security Manager to approve them.

4) Fourth Level: Reports, records, and electronic evidence

The fourth level consists of technical documents that contain the results and conclusions of a study or assessment; technical documents that contain threats and vulnerabilities of information systems, as well as electronic evidence generated during all phases of the information system life cycle.

The responsibility for the existence of this type of documents lies with each of the Information Systems Managers in their area.

5) Other documentation

The STIC procedures, standards and technical instructions, as well as the CCN-STIC guides of the 400, 500, 600 and 800 series, should be followed at all times.

See also UNE-ISO/IEC 27001 and other related regulations.

Regulations, orders, decrees and other legislation relating to the protection of personal data from both the European Union and Spain.

13. Commitment of the Directorate General

The Directorate General of the FGUCM expresses its formal commitment to support the security plans that arise from the application of this Policy. This support will take the form of:

- Providing the necessary human and financial resources, within the limits of economic feasibility;
- Assigning roles and responsibilities to the people associated with the security plans;
- Support the training of human resources involved in security plans so that they acquire the necessary level of awareness and skills;
- Ensure the proper functioning of the Information Security Management System;
- Facilitate communications with other organisations regarding Information Security;
- Promote continuous improvement in the field of Information Security.

Commitment to supporting the plans is expressed by approval of this document.

14. Review and approval

The Information Security Policy will be reviewed at least every two years.

This Information Security Policy was approved by the General Management of the FGUCM in a session held on 2 November 2023.

signature:______________________

Signed: María Paz García Vera

Position: Director General of FGUCM

15. Annex I – Minimum requirements

In order to properly implement and comply with this Security Policy, a series of mandatory requirements must be applied:

15.1 Security in the Organisation

Security must be the responsibility of all members of the FGUCM, without exception.

In Article 6 (Description) of this document, the security organisation is specified via the definition of the organisational structure.

Furthermore, the implementation of this organisation is within the regulatory framework covered by the establishment of a Security Management system, based on the National Security Scheme.

15.2 Risk Analysis and Management

The services and infrastructures under the scope of this Policy must be subject to a risk analysis to guide protection measures aimed at minimising risk.

The description of the methodology and risk assessment are described in ‘Risk analysis and management methodology’.

The risk analysis will also be carried out when personal data processing is to be initiated or modified, as per the provisions of the General Data Protection Regulation. In these cases, all assets involved in the processing will be included in the scope of the analysis, with consideration given to assets related to information systems, as well as human, local or third-party assets.

Based on the results of the aforementioned risk analyses, the measures necessary to protect said data will be determined.

15.3 Personnel management

In section 6.1 of the Human Resources Regulations, on Job Descriptions, the obligation to have knowledge and awareness of security matters is detailed according to responsibilities. The resources required for the implementation of the security system, as well as persons who see to its operation, maintenance and supervision, or are related to the system, are established in the strategic plans of the FGUCM, and are approved by the Steering Committee at the proposal of the Information Security Committee.

The selection of staff is carried out following the criteria set by the Head of Training and Selection of the Personnel Area at the FGUCM.

Performance evaluations and staff monitoring will be periodically conducted by the Data Protection Officer.

15.4 Professionalism

Section 1 of the Human Resources Regulations details the objectives of training and awareness-raising actions, and section 6.2 details the duties and obligations of staff.

A specific training plan is designed every two years, taking into account the professionalisation needs of the security system.

15.5 Authorisation and Access Control

Access to information systems will be restricted and limited to those users or processes that need it in order to carry out their activity and have been previously authorised.

Access to information will follow the 'need to know' principle, so that the privileges granted to each entity are the minimum necessary for the execution of its activity.

User identification will be such that it is possible to know at all times who receives access rights and who has carried out an activity. As such, user identifiers must be personal, not shared, and non-transferable.

Places with restricted access must also be subject to controls and prior authorisation by the assigned persons in charge.

15.6 Protection of the facilities

Information systems must be located in protected areas with access restricted to authorised personnel only. The protection of the facilities is the responsibility of the UCM.

15.7 Product acquisition

For the process of acquiring new products, systems or services, risk analysis protocols are established with suppliers and lists of regular suppliers are kept up to date. Acquisitions should be authorised by the heads of the area concerned and the Supply Area through favourable reports on the supplier, if required.

15.8 Security by Default

Systems and applications will be designed and built under the principle of security by default, in such a way that:

- The system will offer the minimum necessary functionality, and no additional functionality. Any function that is not relevant or is unnecessary will be disabled or not implemented.
- The operation and use of the systems will be limited to authorised persons or locations, and will be prohibited for all others.
- The use of the system must be secure, such that insecure use requires intent on the part of the user.

Security will be present from the conception of a system or application and will remain present throughout its life cycle.

In the design of a new system or application, or substantial modification of an existing system or application, the participation of the Information Security Officer will always be included from the beginning.

15.9 System integrity and updates

Information about vulnerabilities affecting information systems must be monitored at all times.

The recommendations of equipment and software manufacturers regarding security updates shall be followed. Such recommendations should be analysed for their suitability and appropriateness, and if applicable, applied as soon as possible.

15.10 Protection of Information Stored and in Transit

Environments containing stored information and information in transit between insecure environments must be protected. In this regard, portable devices that may contain information, as well as removable media (memory sticks, removable hard drives, etc.), must be adequately secured.

15.11 Prevention against other interconnected information systems.

The necessary protections shall be deployed to protect the perimeter of the FGUCM corporate network. This will be done to neutralise possible intrusions from outside, whether initiated maliciously by third parties or as a result of the connections to third-party systems.

15.12 Activity Log

Systems and applications will generate the necessary activity logs to provide knowledge of the activity in the systems, so that at all times it is possible to determine which person is acting, on which data, with which operations and their access privileges.

15.13 Security Incident Management

FGUCM will define and implement security incident management procedures that ensure proper management and effective response to eliminate or minimise the impact of the incident on information, services, employees, users and, in general, on the activity of FGUCM.

The procedure for managing and responding to security incidents will include the communication and notification of incidents to the organisations receiving said information, in accordance with current legislation.

15.14 Business Continuity

To ensure the availability of services and information systems, FGUCM will design and implement Service Continuity Plans that prevent interruptions in FGUCM activities and guarantee, in the event of a contingency, the resumption of services and information systems at the appropriate levels of operation.

15.15 Security Management and Continuous Improvement

A Security Management System must be established to allow the security status to be known at all times by defining and tracking indicators, and to allow informed decisions to be made to meet the established security requirements.

A continuous improvement process shall be established by analysing the situation, implementing new security measures, improving existing securing measures and the contribution of improvements suggested by the Information Security Committee and by the FGUCM as a whole.